

PURCHASING CARD TRANSACTION RISK MODEL

BACKGROUND OF THE INVENTION

1. Field of the Invention

5 The present invention relates to a method and system for quantifying risk of fraud associated with a purchasing card transaction based on charge-back history associated with a consumer involved in the transaction.

2. Background Art

10 Purchasing cards such as credit cards, department store cards, calling cards, and the like have gained widespread use. Such purchasing cards have many advantages. For example, they allow a consumer or cardholder to make expensive purchases without having large sums of money on hand. Unfortunately, purchasing cards have increasingly become a vehicle to commit fraud. It is estimated that the total cost of purchasing card fraud is \$1.3 million for every 1 million active accounts.

15 At least two conditions must be met before a purchasing card transaction can be completed. First, the cardholder must possess a valid purchasing card. Second, the merchant must be authorized to accept the purchasing card as payment for goods and/or services, and to receive payment from the organization that issued the purchasing card.

20 Typically, purchasing card transactions involve third party purchasing card transaction processors in addition to the merchant and the purchasing card issuer. Transaction processors are typically independent business institutions that provide merchants with data processing services to facilitate the flow of purchasing card transaction data, and the corresponding payment of money, between the
25 merchants and card issuers. The flow of transaction data from the merchant to a card issuer via a transaction processor is commonly referred to as processing or

clearing a transaction. The flow of money from the issuer to the merchant via a processor is known as settlement.

5 For a typical purchasing card transaction, a cardholder presents a purchasing card to a merchant who records the transaction by using an electronic terminal or a manually imprinted sales draft. Alternatively, if the cardholder is making a purchase via the Internet, then the transaction may be recorded via a website. Generally, the recorded data includes purchase amount, the cardholder's account number, expiration date of the purchasing card, and a merchant verification number.

10 Typically, at the end of a particular day, the merchant determines the total dollar volume of the purchasing card transactions completed and prepares a deposit slip indicating the amount. All the transaction data is then transmitted to the merchant's transaction processor, and entered into a computer of the transaction processor. This transfer may be electronic, in which case a data capture terminal
15 may be used to transfer the data directly to the computer of the transaction processor. Alternatively, the transfer may involve the deposit of imprinted paper, such as sales drafts, and subsequent entry of the data into the computer of the transaction processor by data entry personnel.

20 Although purchasing cards provide significant convenience for both cardholders and merchants, there are also well known risks associated with purchasing card transactions. The principal risk is loss resulting from fraudulent or unauthorized use of a purchasing card. Such losses must be absorbed by the merchant, the transaction processor and/or the card issuer.

25 Over the years, card issuers and merchants have relied on several different methods to protect themselves from fraud or misuse, and to verify the validity of a purchasing card before completing a transaction. For example, card issuers may provide "warning bulletins" to merchants. Warning bulletins are booklets that list the account numbers of purchasing cards that should no longer be accepted. Account numbers may be included on these lists if the purchasing card

has been reported lost or stolen, if the cardholder has exceeded his or her credit limit or has become delinquent in payments to the issuer, if the account has experienced excessive charge-backs, or if the purchasing card should not be accepted for another reason (such as mistakenly issued cards and cards that are
5 invalid outside their country of origin).

More recently, card issuers and card issuing associations have provided real-time access to computer databases. This allows merchants to receive telephonic authorization for a transaction based on a search of a continually updated
10 database, which may include similar information as described above with respect to warning bulletins. For a typical transaction authorization, the merchant obtains an authorization code or authorization indicia from an authorization institution or source via telephone or computer terminal. Authorization sources include card
15 issuing associations, card issuers, as well as transaction processors that also provide clearing and settlement services between merchants and card issuers.

Several different methods are currently used for obtaining authorizations. In one method, a merchant uses a telephone to call an authorization source and provide transaction data. An operator associated with the authorization source enters the transaction data into a computer, and provides an authorization
20 number or code to the merchant if the transaction is authorized. Some authorization sources also have audio response units that respond to dual tone multiple frequency signals entered from the merchant's telephone. In this way, the merchant may directly enter numeric transaction data into a computer, and receive an authorization number if the transaction is authorized.

Some transaction processors and card issuers provide an electronic terminal that reads the account number and expiration date from a magnetic strip on the purchasing card. Once the merchant enters the purchased amount into the terminal, the terminal automatically dials an authorization source host computer and initiates an authorization request. The terminal displays and/or stores an
25 authorization code if the transaction is authorized. In each case, the approval code is recorded along with other transaction data.
30

Authorization sources may also provide risk modeling for quantifying risk of fraud associated with purchasing card transactions. Generally, such risk modeling includes evaluating a plurality of factors, and assigning a risk score for a particular transaction that is indicative of the probability that the transaction is fraudulent. The factors that are evaluated may be related to characteristics of the cardholder or purchasing card involved in the transaction, such as last usage, data of issue and card status. Each factor is typically assigned a risk score, and the individual risk scores are combined to obtain an overall risk score. The overall risk score is then forwarded to a requesting merchant, who may then determine whether to complete the transaction.

SUMMARY OF THE INVENTION

The present invention provides a method and system for quantifying risk of fraud based on charge-back history. Consequently, the method and system provide more accurate results than prior art risk-modeling methods and systems.

Under the invention, a method for quantifying risk of fraud associated with a purchasing card transaction includes obtaining a charge-back history associated with a consumer involved in the purchasing card transaction; and determining a risk score based on the charge-back history.

The step of obtaining a charge-back history may include obtaining a reason code for each charge-back included in the charge-back history. Furthermore, the method may include weighting each charge-back included in the charge-back history based on the corresponding reason code. As a result, charge-backs that are more indicative of fraud may be given greater weight than other charge-backs less indicative of fraud, such as a charge-back initiated by a card issuer because the associated merchant failed to timely clear the transaction.

The method may also include obtaining additional charge-back history associated with a machine identification number of a machine involved in the purchasing card transaction. For example, if a personal computer is being used in

the purchasing card transaction, charge-back history associated with an identification number of the computer may be obtained and considered.

5 The step of determining a risk score may be performed in any suitable manner. For example, the risk score may be determined using a linear risk model, a regression risk model, a decision tree risk model, and/or a neural network risk model. Furthermore, other purchasing card transaction characteristics may also be considered, such as card age, card status, card last use, etc.

10 Further under the invention, a system for quantifying risk of fraud associated with a purchasing card transaction includes an authorization source for obtaining a charge-back history associated with a consumer involved in the purchasing card transaction, the authorization source including a risk model for determining a risk score based on the charge-back history.

15 In one embodiment of the system, the authorization source includes a database for storing a reason code for each charge-back included in the charge-back history, and a processor in communication with the database and including the risk model. Furthermore, the risk model includes instructions for determining the risk score based on the reason codes.

20 The above features, benefits and advantages and other features, benefits and advantages of the present invention are readily apparent from the following detailed description of the best mode for carrying out the invention when taken together with the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

FIGURE 1 is a block diagram of a system for conducting a purchasing card transaction in accordance with the present invention; and

FIGURE 2 is a flow diagram illustrating operation of a method, according to the invention, for quantifying risk of fraud associated with a purchasing card transaction.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT(S)

- 5 Before turning to a description of the disclosed embodiments, several terms used throughout this disclosure are defined below in detail.

10 A purchasing card can mean a debit card, a credit card, or other financial account card. Such purchasing cards typically have a magnetic strip carrying an account number associated with the card, expiration date, issuing institution, and other information, as well as a visible indication of an account number and other information in an area of embossed characters. The terms purchasing card, credit card, etc. are used interchangeably hereinafter.

15 A merchant is an institution that renders goods or services in exchange for payment, but also can include other types of institutions that rely upon information provided to them by way of purchasing cards. For example, health service providing institutions that receive information on patients via purchasing cards may be considered merchants.

20 A purchasing card transaction is a transaction typically involving the exchange of information and/or goods and/or services and/or money between a card holding consumer and a goods or services provider, such as a merchant.

25 A transaction processor is an institution that processes purchasing card transactions, for example, a credit card transaction processing company. Transaction processors are sometimes independent third-party institutions that are not related to any particular credit card issuer. However, since many card issuing associations and card issuers also process transactions, card issuing associations and card issuers are generally included within the term transaction processors, except where a distinction between the institutions is required.

A card issuing association is an institution or other entity that issues regulations or requirements governing a particular brand of purchasing card, such as Visa, MasterCard, American Express, Discover, and the like. Some card issuing associations called bank card associations typically include member banks that actually issue credit cards, such as Visa and MasterCard bank card associations. Other non-bank entities, such as American Express, are included within the term for purposes of this invention. Card issuing associations typically accumulate transaction data from transaction processors and send it to particular card issuers.

A card issuer, as used herein, is an institution or organization, often a bank, that issues a purchasing card, such as debit or credit card. Card issuers are generally members of a card issuing association. However, the term card issuer and card issuing association are sometimes used synonymously when the context suggests an entity that is responsible for issuance of purchasing cards as well as regulation of transactions involving purchasing cards.

Settlement refers to the process by which funds are transferred from a card issuer to a merchant.

Clearing a transaction refers to the process by which data pertaining to a merchant's purchasing card transactions are transferred to a card issuer. Transaction clearance is often provided by transaction processors that are independent of a credit card issuer. However, since card issuers may also clear transactions themselves, they are often transaction processors as well.

Authorization indicia, also referred to as authorization codes, authorization approval, or approval code, refers to predetermined signals received from a card issuing association, or other authorization source, that indicate that a particular transaction has been authorized. These indicia may be electronic or may be audible. Furthermore, these indicia are generally associated with other transaction data to flag the transaction as having been pre-approved.

Referral means a signal or predetermined indicia received by a merchant from an authorization source indicative that the merchant should contact the authorization source or a card issuer in connection with a particular transaction. A referral is often generated in response to a determination that a particular purchasing card should not be accepted for various reasons, such as the card holder has exceeded his or her credit limit, the purchasing card has been stolen, or for some other reason.

An audio response unit or ARU is a synthesized voice generating apparatus that responds to dual tone multiple frequency (DTMF) signals provided by a standard touch-tone telephone to enter the account number, expiration date and purchase amount. In addition, the ARU contains circuitry that is capable of recognizing certain spoken words and numbers. If a transaction is approved, the ARU's voice synthesizer provides an approval number and is operative for generating an audible but synthesized voice and message corresponding to a predetermined message. For example, an ARU may be programmed to provide messages, such as transaction authorized, approval code is 12345, or transaction declined. Such messages are generated and relayed to the merchants automatically and telephonically without human intervention or participation.

A retrieval request is a request or inquiry made of a merchant or a merchant's transaction processor, typically from a card holder or card issuer, for a hard copy of documentation associated with a given transaction. Typically a transaction may be charged back to the transaction processor or merchant if the requested documentation is not provided within a time limit set under card issuing association regulations.

Referring now to Figure 1, an overview of a system 10 according to the present invention for processing and settling purchasing card transactions is illustrated. Such purchasing card transactions may include any transaction involving a purchasing card, such as a mail-order transaction, telephone-order transaction, electronic transaction initiated over the Internet, and/or a transaction initiated at a merchant location. Generally, a consumer, such as cardholder 12, who desires to

purchase goods and/or services, provides a purchasing card or an account number associated with the purchasing card to a merchant 14 as a method of payment. The merchant 14 communicates with an authorization source 16 to request transaction authorization and a risk assessment for quantifying the risk of fraud associated with the particular transaction.

The Authorization source 16 preferably includes a computer system having necessary hardware and/or software for authorizing the transaction and for performing the risk assessment. For example, authorization source 16 may have a processor, such as a microprocessor 17, that includes necessary instructions for authorizing the transaction and for performing the risk assessment. Authorization source 16 may also communicate with one or more card issuing associations, such as card issuing association 18, and/or one or more card issuers, such as card issuer 20, so as to obtain information for determining whether to authorize the transaction and/or for performing the risk assessment. The Authorization source 16 may also obtain information from an internal database 21 and/or one or more external databases 22 for use in performing the risk assessment, as explained below in greater detail.

The authorization source 16 may be an independent institution, a card issuing association, a card issuer, and/or a transaction processor. Some merchants may also function as their own authorization source. Furthermore, it should be understood that one authorization source may be used to obtain transaction authorization, and another authorization source may be used to obtain the risk assessment.

If the transaction is approved, the authorization source 16 may provide the merchant 14 an authorization number. In response to the authorization request, the merchant 14 may instead receive a decline, in which case the transaction is terminated, or a referral, in the event the authorization source 16 requires more information before authorizing the transaction.

After performing the risk assessment, the authorization source 16 may also provide the merchant 14 an overall risk score, which represents the likelihood that the transaction is fraudulent. The merchant 14 may then use the overall risk score to determine whether or not to proceed with the transaction.

5 Generally, the merchant 14 uses an electronic terminal, such as an ARU described above, or any other suitable terminal, to communicate with the authorization source 16 and to record transaction data pertaining to the transaction. The transaction data may include the account number and expiration date associated with the purchasing card, the amount and date of the purchase, the authorization
10 number, the overall risk score, and the cardholder's signature.

Typically, the merchant transfers the transaction data to a transaction processor 23 at the end of the day, along with other transaction data from other transactions that occurred during the day, so that the transactions may be processed or cleared. Transaction processor 23 separates the transaction data according to
15 type of purchasing card, and forwards the transaction data to card issuing association 18, or other appropriate card issuing associations. The card issuing association 18 accumulates transaction data and sends it to the card issuer 20, or other appropriate card issuers. Once card issuer 20 receives the transaction data associated with the transaction described above, the transaction is posted to the
20 cardholder's account, and a statement or bill 24 is sent to the cardholder 12.

Referring to Figures 1 and 2, an overview of a risk assessment conducted by authorization source 16 in connection with a purchasing card transaction will now be described. First, merchant 14 requests transaction authorization and a risk assessment from the authorization source 16, as represented
25 by block 26. At block 28, merchant 14 transmits purchasing card information associated with the purchasing card to the authorization source 16. Such purchasing card information may include the account number and expiration date associated with the purchasing card, the amount and date of the purchase, and/or other information. Authorization source 16 then retrieves or otherwise obtains a plurality
30 of transaction characteristics, such as risk factors, from internal database 21 of

authorization source 16, and/or from one or more external databases 22, as indicated at step 30. Such risk factors may include charge-back history, card age, card status, card last use, card watch list, etc., and are preferably stored at least temporarily on the internal database 21.

5 Charge-back history includes information on charge-backs associated with cardholder 12. For example, charge-back history may include information on charge-backs associated with the purchasing card being used in the current transaction and/or charge-backs associated with another purchasing card for which the cardholder 12 is an authorized user. As another example, charge-back history
10 may include information on charge-backs associated with an address, telephone number and/or e-mail address of the cardholder 12. Charge-back history may also include information on charge-backs otherwise associated with the cardholder 12 and/or other aspects of the transaction, such as a ship to address, a telephone number of a telephone that is used to initiate the transaction (which may be captured
15 or otherwise obtained by a caller identification device), or a machine identification number. For instance, if the cardholder 12 is attempting to purchase products or services over the Internet using a personal computer, authorization source 16 may capture the machine identification number of the personal computer and then obtain charge-back history associated with the identification number.

20 A charge back occurs when a card issuing association or card issuer refuses to honor a particular transaction, and results in reversal of the transaction to a transaction processor or merchant. For example, a cardholder may request a charge back if a particular transaction was not authorized by the cardholder, or if the product or service was not provided in accordance with the sale terms. As
25 another example, the card issuing association or card issuer may automatically charge back a particular transaction if the merchant failed to clear the transaction in a timely manner.

Charge-back history preferably includes the number of charge-backs, the dollar amount of each charge-back, and a reason code for each charge-back
30 associated with the cardholder 12 and/or other aspect of the transaction. The reason

code is a code, such as a number, letter or alpha-numeric symbol, that indicates the reason for the charge-back. For example, the reason code may indicate that the cardholder 12 was dissatisfied with a previously purchased product or service, or that the cardholder 12 never ordered the product or service. As another example,

5 the reason code may indicate that a purchasing card association or card issuer charged back a particular transaction because the merchant failed to clear the transaction in a timely manner.

Card age is defined as the length of time the account number associated with the purchasing card has been stored in internal database 21 of the

10 authorization source 16, or in an external database 22. Typically, the lower the card age is, the greater the likelihood that the transaction involves fraud.

Card status is the current status of the purchasing card as recorded in internal database 21 of the authorization source 16, or in an external database 22. For example, the card status may be "retrieval issued". A retrieval is a request for

15 information regarding a transaction from a card issuer. Other card statuses may include "consumer block" or "system block". A "consumer block" may be requested by a cardholder so as to block certain transactions, and a "system block" is typically requested by a card issuing association or card issuer so as to block all transactions.

20 Card last use is the date and time the purchasing card, or the account number associated with the purchasing card, was last used in a transaction. Depending on certain factors, such as transaction type and transaction amount, a recent card last use, for example, may indicate a high probability of transaction fraud.

25 A card watch list is a listing of purchasing card account numbers that have been reported stolen or are known to be involved in fraudulent activity. Other watch lists, such as a country watch list or an Internet Protocol (IP) watch list may also be obtained and reviewed. A country watch list is a listing of cardholder names and/or purchasing account numbers that have been involved in fraudulent activity

in one or more countries. An IP watch list is a listing of cardholder names and/or purchasing account numbers that have been involved in fraudulent activity on one or more web sites.

5 The authorization source 16, having the current purchasing card information and the risk factors retrieved from the internal and/or external databases 21 and 22, respectively, then performs a risk assessment to quantify risk of fraud associated with the purchasing card transaction, as represented by block 32. The risk assessment may be performed in any suitable manner, such as by using a linear risk model, a regression risk model, a decision tree risk model, a neural network risk model, and/or any other suitable risk model. Furthermore, the authorization source 16 may include a plurality of such risk models, which are preferably contained on suitable hardware and/or software. For example, the microprocessor 10 17 of the authorization source 16 may include all instructions necessary for executing one or more risk models.

15 The risk assessment involves evaluating the risk factors identified above, and assessing or otherwise determining an overall risk score, as represented by block 34. The overall risk score represents the likelihood that the transaction is fraudulent, or will later become fraudulent. In one embodiment of the invention, the higher the overall risk score, the greater the likelihood that the transaction is fraudulent. For example, the overall risk score may be a number ranging from zero 20 to ten, where zero represents the lowest likelihood that the transaction is fraudulent, and where ten represents the highest likelihood that the transaction is fraudulent.

25 With respect to charge-back history, the risk assessment may involve considering the reason code for each charge-back in order to determine what weight should be given to each charge-back. For example, if the reason code for a particular charge-back indicates that a purchasing card association or card issuer initiated the charge-back, then the charge-back may be assigned relatively little weight or disregarded. As another example, a charge-back having a reason code that indicates dissatisfaction with a product or service may be given more weight

than a charge-back having a reason code that indicates that the cardholder never ordered a particular product or service.

Alternatively or supplementally, the risk assessment may involve considering how each charge-back is associated with the current transaction in order to determine what weight should be given to each charge-back. For example, a charge-back associated with a telephone number of a telephone that is being used to initiate the current transaction may be given more weight than a charge-back associated with a ship to address.

At block 36, the overall risk score for the purchasing card transaction is transmitted to the merchant 14, who may then make a determination as to whether or not to proceed with the transaction. Alternatively, the authorization source 16 may determine that the transaction should be declined based on the overall risk score. In this case, the authorization source 16 may transmit a message or indicia indicating to the merchant 14 that the transaction should be declined or is not authorized.

Because the risk assessment involves evaluating charge-back history, the system and method of the present invention provide more accurate results than prior art systems and methods. Advantageously, the risk assessment may also be modified based on the type of product or service involved in the transaction, and/or based on how the transaction is being performed, e.g., in store purchase, mail order, telephone order, purchase over the Internet, etc. For example, if the transaction involves adult material, such as products or services that are restricted from being sold to persons under the age of 18, or other age set by applicable law, then certain risk factors may be scored differently and/or weighted differently.

With reference to Table 1 shown below, an example of how an overall risk score may be assessed or scored, based on a linear risk model, will now be described. In column A of Table 1, a plurality of risk factors used to determine the risk of a fraudulent transaction are listed. In column B of Table 1, a scoring range for each risk factor is provided. Finally, in column C, an assessed risk score

is shown for each risk factor associated with a particular transaction. The risk scores shown in column C are then summed and an overall risk score is determined.

TABLE 1

A	B	C
RISK FACTOR	SCORE RANGE	CURRENT SCORE
Card Age	0-10	8
Card Status	1-10	2
Card Last Use	1-10	1
Card Watch List	0 or 10	0
Charge back history	1-10	5
	OVERALL SCORE	3.2

The first risk factor shown in Table 1 is "Card Age". The card age for a particular purchasing card may fall within one of a plurality of ranges, such as zero to seven days, seven to thirty days, thirty to sixty days, etc. Each range may have an associated risk score that indicates the riskiness of a transaction. The higher the risk score, the higher the probability that the transaction is fraudulent. For instance, if the card age falls within a range of zero to seven days, a high risk score may be assessed, such as a ten. If the card age falls within a range of seven to thirty days, then a lower risk score, such as eight, may be assigned.

The next risk factor shown in Table 1 is "Card Status", which is scored according to the current status of the purchasing card in a particular database. For example, a card status of "retrieval issued" may be assigned a risk score of two. Other card statuses such as "consumer block" and "system block" may be assigned risk scores of seven and ten, respectively. A transaction involving a purchasing card having a status of "consumer block" or "system block" is considered to have a higher likelihood of being fraudulent than a transaction involving a purchasing card having a status of "retrieval issued". Thus, the

assigned risk scores for "consumer block" and "system block" are typically higher than for "retrieval issued".

5 "Card Last Use" is the next risk factor shown in Table 1. If the last use of the purchasing card is very recent, such as within the last minute or hour, then the potential that the transaction is fraudulent may be high. As a result, a risk score of ten may be assigned. However, if the last use of the purchasing card is not recent, such as within the last month, then the potential that the transaction is fraudulent may be low. As a result, a risk score of one may be assigned.

10 The next risk factor shown in Table 1 is "Card Watch List". If the purchasing card account number is on a card watch list because the associated purchasing card was previously used in a fraudulent transaction, then the potential that the current transaction is fraudulent is high. As a result, a risk score of ten may be assigned. However, if the purchasing card is not on the card watch list, then the
15 potential that the transaction is fraudulent is low. As a result, a risk score of zero may be assigned.

The last risk factor shown in Table 1 is "Charge-back History". If, for example, the purchasing card account number involved in the current transaction has an extensive charge-back history, then the potential that the current transaction
20 is fraudulent is considered to be high. As a result, a risk score of ten may be assigned. However, if the purchasing card account number has little to no charge-back history, then the potential that the current transaction is fraudulent is considered to be low. As a result, a risk score of one may be assigned.

25 As mentioned above, other charge-backs associated with the cardholder 12, such as charge-backs associated with the name, address and/or telephone number of the cardholder 12, may also be obtained and considered. Furthermore, charge-backs associated with other aspects of the transaction, such as charge-backs associated with a ship to address and/or telephone number of a
30 telephone that is being used to initiate the transaction, may also be obtained and considered.

5 The reason code associated with each charge-back may also be considered in order to determine what weight should be given to each charge-back. For example, a charge-back having a reason code that indicates fraud, may be weighted twice as much as a charge-back having a reason code that indicates that the cardholder was dissatisfied with a purchased product or service.

10 Alternatively or supplementally, the association between each charge-back and the current transaction may also be considered in order to determine what weight should be given to each charge-back. For example, a charge-back associated with a telephone number of a telephone that is being used to initiate the current transaction (which telephone number may be captured by a caller identification device), may be weighted fifty percent more than a charge-back associated with a telephone number provided by the cardholder 12. Furthermore, this weighting may occur before or after weighting based on reason code.

15 After the charge-backs have been properly weighted, the total number of charge-backs may be compared to predetermined ranges to determine the associated risk score. For example, a range of two to three charge-backs may be assigned a risk score of five, and a range of four to five charge-backs may be assigned a risk score of six.

20

Many other risk factors, of course, can be used to assess the potential that a particular purchasing card transaction is fraudulent. Additional risk factors can be evaluated and scored in a similar manner as described above in detail.

25 The overall risk score may be determined based on the risk scores for the risk factors. For example, the overall risk score may be calculated by summing all of the individual scores for the risk factors, and then dividing by the total number of risk factors. Thus, for the example illustrated in Table 1, the overall risk score is 3.2.

Alternatively, the individual risk scores may be weighted differently. For example, the risk score for card watch list or charge-back history may be doubled prior to computing the overall risk score.

- 5 While embodiments of the invention have been illustrated and described, it is not intended that these embodiments illustrate and describe all possible forms of the invention. Rather, the words used in the specification are words of description rather than limitation, and it is understood that various changes may be made without departing from the spirit and scope of the invention.

11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000
1001
1002
1003
1004
1005
1006
1007
1008
1009
1010
1011
1012
1013
1014
1015
1016
1017
1018
1019
1020
1021
1022
1023
1024
1025
1026
1027
1028
1029
1030
1031
1032
1033
1034
1035
1036
1037
1038
1039
1040
1041
1042
1043
1044
1045
1046
1047
1048
1049
1050
1051
1052
1053
1054
1055
1056
1057
1058
1059
1060
1061
1062
1063
1064
1065
1066
1067
1068
1069
1070
1071
1072
1073
1074
1075
1076
1077
1078
1079
1080
1081
1082
1083
1084
1085
1086
1087
1088
1089
1090
1091
1092
1093
1094
1095
1096
1097
1098
1099
1100
1101
1102
1103
1104
1105
1106
1107
1108
1109
1110
1111
1112
1113
1114
1115
1116
1117
1118
1119
1120
1121
1122
1123
1124
1125
1126
1127
1128
1129
1130
1131
1132
1133
1134
1135
1136
1137
1138
1139
1140
1141
1142
1143
1144
1145
1146
1147
1148
1149
1150
1151
1152
1153
1154
1155
1156
1157
1158
1159
1160
1161
1162
1163
1164
1165
1166
1167
1168
1169
1170
1171
1172
1173
1174
1175
1176
1177
1178
1179
1180
1181
1182
1183
1184
1185
1186
1187
1188
1189
1190
1191
1192
1193
1194
1195
1196
1197
1198
1199
1200
1201
1202
1203
1204
1205
1206
1207
1208
1209
1210
1211
1212
1213
1214
1215
1216
1217
1218
1219
1220
1221
1222
1223
1224
1225
1226
1227
1228
1229
1230
1231
1232
1233
1234
1235
1236
1237
1238
1239
1240
1241
1242
1243
1244
1245
1246
1247
1248
1249
1250
1251
1252
1253
1254
1255
1256
1257
1258
1259
1260
1261
1262
1263
1264
1265
1266
1267
1268
1269
1270
1271
1272
1273
1274
1275
1276
1277
1278
1279
1280
1281
1282
1283
1284
1285
1286
1287
1288
1289
1290
1291
1292
1293
1294
1295
1296
1297
1298
1299
1300
1301
1302
1303
1304
1305
1306
1307
1308
1309
1310
1311
1312
1313
1314
1315
1316
1317
1318
1319
1320
1321
1322
1323
1324
1325
1326
1327
1328
1329
1330
1331
1332
1333
1334
1335
1336
1337
1338
1339
1340
1341
1342
1343
1344
1345
1346
1347
1348
1349
1350
1351
1352
1353
1354
1355
1356
1357
1358
1359
1360
1361
1362
1363
1364
1365
1366
1367
1368
1369
1370
1371
1372
1373
1374
1375
1376
1377
1378
1379
1380
1381
1382
1383
1384
1385
1386
1387
1388
1389
1390
1391
1392
1393
1394
1395
1396
1397
1398
1399
1400
1401
1402
1403
1404
1405
1406
1407
1408
1409
1410
1411
1412
1413
1414
1415
1416
1417
1418
1419
1420
1421
1422
1423
1424
1425
1426
1427
1428
1429
1430
1431
1432
1433
1434
1435
1436
1437
1438
1439
1440
1441
1442
1443
1444
1445
1446
1447
1448
1449
1450
1451
1452
1453
1454
1455
1456
1457
1458
1459
1460
1461
1462
1463
1464
1465
1466
1467
1468
1469
1470
1471
1472
1473
1474
1475
1476
1477
1478
1479
1480
1481
1482
1483
1484
1485
1486
1487
1488
1489
1490
1491
1492
1493
1494
1495
1496
1497
1498
1499
1500
1501
1502
1503
1504
1505
1506
1507
1508
1509
1510
1511
1512
1513
1514
1515
1516
1517
1518
1519
1520
1521
1522
1523
1524
1525
1526
1527
1528
1529
1530
1531
1532
1533
1534
1535
1536
1537
1538
1539
1540
1541
1542
1543
1544
1545
1546
1547
1548
1549
1550
1551
1552
1553
1554
1555
1556
1557
1558
1559
1560
1561
1562
1563
1564
1565
1566
1567
1568
1569
1570
1571
1572
1573
1574
1575
1576
1577
1578
1579
1580
1581
1582
1583
1584
1585
1586
1587
1588
1589
1590
1591
1592
1593
1594
1595
1596
1597
1598
1599
1600
1601
1602
1603
1604
1605
1606
1607
1608
1609
1610
1611
1612
1613
1614
1615
1616
1617
1618
1619
1620
1621
1622
1623
1624
1625
1626
1627
1628
1629
1630
1631
1632
1633
1634
1635
1636
1637
1638
1639
1640
1641
1642
1643
1644
1645
1646
1647
1648
1649
1650
1651
1652
1653
1654
1655
1656
1657
1658
1659
1660
1661
1662
1663
1664
1665
1666
1667
1668
1669
1670
1671
1672
1673
1674
1675
1676
1677
1678
1679
1680
1681
1682
1683
1684
1685
1686
1687
1688
1689
1690
1691
1692
1693
1694
1695
1696
1697
1698
1699
1700
1701
1702
1703
1704
1705
1706
1707
1708
1709
1710
1711
1712
1713
1714
1715
1716
1717
1718
1719
1720
1721
1722
1723
1724
1725
1726
1727
1728
1729
1730
1731
1732
1733
1734
1735
1736
1737
1738
1739
1740
1741
1742
1743
1744
1745
1746
1747
1748
1749
1750
1751
1752
1753
1754
1755
1756
1757
1758
1759
1760
1761
1762
1763
1764
1765
1766
1767
1768
1769
1770
1771
1772
1773
1774
1775
1776
1777
1778
1779
1780
1781
1782
1783
1784
1785
1786
1787
1788
1789
1790
1791
1792
1793
1794
1795
1796
1797
1798
1799
1800
1801
1802
1803
1804
1805
1806
1807
1808
1809
1810
1811
1812
1813
1814
1815
1816
1817
1818
1819
1820
1821
1822
1823
1824
1825
1826
1827
1828
1829
1830
1831
1832
1833
1834
1835
1836
1837
1838
1839
1840
1841
1842
1843
1844
1845
1846
1847
1848
1849
1850
1851
1852
1853
1854
1855
1856
1857
1858
1859
1860
1861
1862
1863
1864
1865
1866
1867
1868
1869
1870
1871
1872
1873
1874
1875
1876
1877
1878
1879
1880
1881
1882
1883
1884
1885
1886
1887
1888
1889
1890
1891
1892
1893
1894
1895
1896
1897
1898
1899
1900
1901
1902
1903
1904
1905
1906
1907
1908
1909
1910
1911
1912
1913
1914
1915
1916
1917
1918
1919
1920
1921
1922
1923
1924
1925
1926
1927
1928
1929
1930
1931
1932
1933
1934
1935
1936
1937
1938
1939
1940
1941
1942
1943
1944
1945
1946
1947
1948
1949
1950
1951
1952
1953
1954
1955
1956
1957
1958
1959
1960
1961
1962
1963
1964
1965
1966
1967
1968
1969
1970
1971
1972
1973
1974
1975
1976
1977
1978
1979
1980
1981
1982
1983
1984
1985
1986
1987
1988
1989
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025
2026
2027
2028
2029
2030
2031
2032
2033
2034
2035
2036
2037
2038
2039
2040
2041
2042
2043
2044
2045
2046
2047
2048
2049
2050
2051
2052
2053
2054
2055
2056
2057
2058
2059
2060
2061
2062
2063
2064
2065
2066
2067
2068
2069
2070
2071
2072
2073
2074
2075
2076
2077
2078
2079
2080
2081
2082
2083
2084
2085
2086
2087
2088
2089
2090
2091
2092
2093
2094
2095
2096
2097
2098
2099
2100
2101
2102
2103
2104
2105
2106
2107
2108
2109
2110
2111
2112
2113
2114
2115
2116
2117
2118
2119
2120
2121
2122
2123
2124
2125
2126
2127
2128
2129
2130
2131
2132
2133
2134
2135
2136
2137
2138
2139
2140
2141
2142
2143
2144
2145
2146
2147
2148
2149
2150
2151
2152
2153
2154
2155
2156
2157
2158
2159
2160
2161
2162
2163
2164
2165
2166
2167
2168
2169
2170
2171
2172
2173
2174
2175
2176
2177
2178
2179
2180
2181
2182
2183
2184
2185
2186
2187
2188
2189
2190
2191
2192
2193
2194
2195
2196
2197
2198
2199
2200
2201
2202
2203
2204
2205
2206
2207
2208
2209
2